**ANÁLISIS DE RIESGOS INFORMÁTICOS**

Como bien podemos ver, todo este proceso se orienta al objetivo de [establecer estrategias adecuadas](https://www.gb-advisors.com/es/tech-blog-es/asesoria-en-herramienta-itsm/) para mitigar los riesgos informáticos; el cual sigue siendo una de las principales preocupaciones de las empresas en materia de seguridad digital. Asimismo, le siguen de cerca la creación de controles; preservación de la integridad y confidencialidad de datos; y la disponibilidad de recursos.

* Identificación o inventario de activos sensibles de vulnerabilidades y amenazas.
* Vulnerabilidades y amenazas comunes a las que se expone la compañía.
* Cálculo de probabilidades en las que estas últimas puedan atacar los activos.
* Posibles impactos de las mismas sobre las operaciones.

SEGURIDAD DIGITAL DE CARA A LA GESTIÓN DE VULNERABILIDADES

instruir a los empleados en la creación de [claves y contraseñas seguras](https://www.gb-advisors.com/es/tech-blog-es/fallas-de-seguridad-en-sistemas/) en conjunto con otras prácticas centradas en el usuario

PERÍODO DE DIAGNÓSTICO Y EVALUACIÓN DE RIESGOS INFORMÁTICOS

 Este período se caracteriza por estar sujeto al cumplimiento de variables adicionales tales como presupuesto; experiencia; personal a disposición; conocimientos técnicos; planes de recuperación de eventos de seguridad; protocolo de actualizaciones; etc.

### MISCELÁNEO DE ACTIVIDADES POSTERIORES AL PROCESO DE DIAGNÓSTICO DE RIESGOS INFORMÁTICO

Desde luego, el ciclo del diagnóstico de riesgos informáticos tiene un fin. Dicha fase compila un misceláneo de actividades pensadas para la corrección y seguimiento a la vigencia de las medidas de seguridad resultantes del diagnóstico.

Tales actividades misceláneas incluye la aplicación de parches; instalación de actualizaciones; gestión del ciclo de vida de sistemas y herramientas de seguridad; actividades para el reemplazo por Fin de Vida Útil; etc.

